UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AFIF TAI and JOSEPH COLLINS, individually and on behalf of all others similarly situated, Plaintiffs, v. NEW YORK UNIVERSITY, Defendant.	Case No.: **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiffs Afif Tai and Joseph Collins ("Plaintiffs"), individually and on behalf all others similarly situated, bring this action against Defendant New York University ("NYU" or "Defendant"), seeking monetary damages, restitution, and/or injunctive relief for the proposed Class, as defined below. Plaintiffs make the following allegations upon information and belief, the investigation of counsel, and personal knowledge or facts that are a matter of public record.

I. INTRODUCTION

1. The release, disclosure, and publication of sensitive, private data can be devastating. Not only is it an intrusion of privacy and a loss of control, but it is a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.[1] A data breach can have grave consequences for victims for years after the actual date of the breach – with the obtained information, thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain medical services, obtain government benefits, and/or obtain driver's licenses

[1] Dave Maxfield & Bill Latham, *Data Breaches: Perspectives from Both Sides of the Wall*, 25 S.C. Lawyer 28-35 (May 2014), https://www.mydigitalpublication.com/publication/?i=208503 (last accessed Mar. 27, 2025).

in the victims' names, forcing victims to maintain a constant vigilance over the potential misuse of their information.

2. New York University, based in New York City, is one of America's largest elite private academic institutions. Founded in 1831, the university boasts an enrollment of over 60,000 students spread across three campuses in New York, Abu Dhabi, and Shanghai, along with 12 global academic centers.[2] Supported by a nearly $5 billion endowment, the university has ample resources and is one of the largest employers in New York City with more than 19,000 employees.[3]

3. NYU remains overwhelmingly popular with high school students looking to attend college and acceptance is competitive: in 2023, the university received over 100,000 applications with a 13% acceptance rate.[4] These applications contain highly sensitive Personally Identifiable Information ("PII"), including names, addresses, financial background data, and information related to the applicant's family members. Due to the nature of the university's reputation and desirability, NYU receives, handles, and maintains the PII of millions of hopeful students throughout the world. On information and belief, all information related to these applicants and their family members are contained within and stored in NYU's databases and information systems.

4. On March 22, 2025, a hacker took over NYU's website and exposed the PII of over three million applicants to the university (the "Data Breach").[5] Accusing NYU of using "illegal" affirmative action admissions policies, the hacker posted four accessible CSV files with NYU admissions data going back to at least 1989, which included "over 3 million admitted students' applications, demographic data, city and zip codes and citizenship status."[6] Additionally, the files

---

[2] NYU, "Admissions," https://www.nyu.edu/admissions.html (last accessed Mar. 27, 2025).
[3] NYU, "NYU At a Glance," https://www.nyu.edu/news-publications/nyu-at-a-glance.html (last accessed Mar. 27, 2025).
[4] *Id.*
[5] Dharma Niles, Krish Dev, and Yezen Saadah, "Over 3 Million Applicants' Data Leaked on NYU's Website," Washington Square News, Mar. 22, 2025, https://www.nyunews.com/news/2025/03/22/nyu-website-hacked-data-leak/ (last accessed Mar. 27, 2025).
[6] *Id.*

revealed data involving rejected students, financial aid, and personal information about family members.

5. Despite knowing how valuable the information of both rejected and admitted students is, NYU failed to adequately protect Plaintiffs' and Class Members' PII. NYU was aware of the risks of data breaches, as numerous peer institutions, including Georgetown University and Stanford University, have been attacked and breached for their respective student information in recent years.[7] NYU also took no steps to minimize the risk of harm to its former applicants, as it kept applications for decades, even though it had no genuine need to do so and apparently did not encrypt these files. The hacker committing this Data Breach also claimed responsibility on X for a similar incident at the University of Minnesota in 2023.[8]

6. Plaintiffs' and Class Members' PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect applicants' sensitive data. The hacker targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting, stealing, and exposing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

7. As a result of the Data Breach, through which their PII was compromised, disclosed, and obtained by unauthorized third parties, Plaintiffs and Class Members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud and identity theft for a period of years, if not decades. Furthermore, Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft, at their own expense. Consequently, Plaintiffs and the other Class Members will incur ongoing out-of-pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

---

[7] *Id.*

[8] Rikki Schlott and Chris Harris, "Hacker claims responsibility for replacing NYU's website with apparent test scores, racial epithet," NY Post, Mar. 22, 2025, https://www.nypost.com/2025/03/22/us-news/ny-us-website-seemingly-hacked-and-replaced-by-apparent-test-scores-racial-epithet/ (last accessed Mar. 27, 2025).

8. By this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

II. JURISDICTION & VENUE

9. This Court has subject matter jurisdiction for this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1711, et seq., because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs. This Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 and supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. § 1367. This Court also has diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a).

10. The Court has jurisdiction over Defendant because Defendant maintains its principal place of business in this District, has sufficient minimum contacts with this District, and has purposefully availed itself of the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District.

11. Venus is proper in this District under 28 U.S.C. § 1391(a) through (d) because Defendant's principal place of business is located in this District and a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

III. PARTIES

A. Plaintiff Afif Tai

12. Plaintiff Afif Tai is a resident of Queens, New York.

13. Plaintiff Tai applied to NYU in 2021 and also submitted an application for financial aid.

B. Plaintiff Joseph Collins

14. Plaintiff Joseph Collins is a resident of Los Angeles, California.

15. Plaintiff Collins applied to NYU in 2017 and also submitted an application for financial aid.

16. Plaintiff Collins matriculated from NYU in 2021.

C. Defendant

17. Defendant New York University is a private academic institution with its principal place of business at 50 West 4th Street, New York, New York 10012.

IV. FACTUAL ALLEGATIONS

D. New York University Failed to Adequately Protect Student Applicant Data, Resulting in the Data Breach

18. NYU's own privacy policy states that it has "implemented reasonable physical, technical, and administrative procedures to safeguard and secure all information we collect online against loss, misuse, or alteration of the information under our control."[9] Notwithstanding these promises, in March 2025, NYU experienced a data breach affecting roughly three million applicants. Upon information and belief, the hacker gained access to Plaintiffs and Class Members' PII with the intent of publicly distributing and misusing this PII to expose NYU's admission processes.

19. While NYU provided a statement to their student newspaper that the university "reported the hack to law enforcement, is taking steps to make sure the attackers are out of our systems, and is reviewing [our systems] to bolster their security," NYU has yet to personally notify applicants as to whether their information was leaked in the breach.[10] Plaintiffs and Class

[9] NYU, "Digital Privacy Statement," https://www.nyu.edu/footer/copyright-and-fair-use/digital-privacy-statement.html (last accessed Mar. 27, 2025).
[10] Niles at *2.

Members remain in the dark regarding what specific PII was stolen, the malware used, and the steps taken to secure their PII moving forward.

20. Defendant was familiar with its obligations – to protect student and applicant information. Plaintiffs and Class Members have provided their private information to NYU with the reasonable expectation that Defendant would comply with its obligations related to their PII. NYU owed Plaintiffs and Class Members a duty to provide reasonable security, consistent with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected their PII.

21. NYU could have taken steps to minimize the harm that would flow from the Data Breach. It could have deleted admission files that it no longer needed and it could have encrypted the valuable information of applicants.

22. Despite these duties, Defendant failed to comply with its obligations, resulting in the Data Breach and Class Members now face years of constant surveillance of their financial and personal records.

E. The Data Breach Puts Class Members at Increased Risk of Fraud and Identity Theft

23. An identity thief often uses victims' PII, such as name, address, and other sensitive and confidential information, without permission, to commit fraud or other crimes that range from immigration fraud, obtaining a driver's license or identification card, obtaining government benefits, and filing fraudulent tax returns to obtain tax refunds.

24. Identity thieves can use a victim's PII to open new financial accounts, incur charges in the victim's name, take out loans in the victim's name, and incur charges on existing accounts of the victim. Plaintiffs' and Class Members' finances are now at risk due to the Data Breach.

25. Identity theft is the most common consequence of a data breach – it occurs to 65%

of data breach victims.[11] Consumers lost more than $56 billion to identity theft and fraud in 2020, and over 75% of identity theft victims reported emotional distress.[12] Victims of identity theft can experience financial damage as thieves run up debts into the tens of thousands. These victims can have their credit history destroyed, impairing their ability to obtain a loan, a mortgage, or even to lease housing. Victims of identity theft can experience substantial legal complications due to breaches. These risks and vulnerabilities are ongoing.

26. Plaintiffs and members of the Class are now in the position of having to take steps to mitigate these damages caused by the Data Breach. Once the use of compromised non-financial PII is detected, the emotional and economic consequences to the victims are significant. Studies done by the ID Theft Resource Center, a non-profit organization, found that victims of identity theft had marked increased fear for personal financial security. The report attributes this to more people having been victims before, contributing to greater awareness and understanding that they may suffer long-term consequences from this type of crime.[13]

27. Defendant failed to protect and safeguard Plaintiffs' and Class Members' private information, in fact failing to adhere to even its most basic obligations. As a result, Plaintiffs and Class Members have suffered or will suffer actual injury, including loss of privacy, costs and loss of time.

V. CLASS ACTION ALLEGATIONS

28. Plaintiffs bring this action as a class action under Rule 23 of the Federal Rules of

[11] Eugene Bekker, *What Are Your Odds of Getting Your Identity Stolen?*, IDENTITYFORCE (Apr. 15, 2021), https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics (last accessed Mar. 27, 2025).
[12] *Id.*
[13] Identity Theft: The Aftermath 2013, Identity Theft Resource Center, https://www.idtheftcenter.org/wp-content/uploads/2021/09/Aftermath2013.pdf (last accessed Mar. 27, 2025).

Civil Procedure, on behalf of a proposed class (the "Class"), defined as:

> **Nationwide Class:** All natural persons in the United States whose Personally Identifiable Information was compromised as a result of the Data Breach.

29. In addition, the California Subclass is defined as follows:

> **California Subclass:** All natural persons who were residents of California at the time of the Data Breach and whose Personally Identifiable Information was compromised as a result of the Data Breach.

30. Excluded from the Class are Defendant, any entity in which a Defendant has a controlling interest, any of the officers or directors of Defendant, the legal representatives, heirs, successors, and assigns of Defendant, and any Judge to whom this case is assigned, and his or her immediate family.

31. The definition of the Class may be further modified or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

32. **Numerosity and Ascertainability:** Plaintiffs do not know the exact size of the Class or the identity of the Class Members because such information is in the exclusive control of Defendant. Nevertheless, based on published reports, the Class comprises millions of applicants throughout the United States. The Class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties and the Court. The names, phone numbers, and addresses of Class Members are identifiable through documents maintained by Defendant.

33. **Commonality and Predominance:** This action involves common questions of law and fact as to all members of the class, which predominate over any question solely affecting individual Class Members. Common questions of law and fact include, but are not limited to, the following:

a) Whether Defendant engaged in the conduct alleged herein;
b) Whether Defendant had a legal duty to use reasonable security measures to protect Plaintiffs' and Class Members' PII;
c) Whether Defendant's failure to implement effective security measures to protect Class Members' PII was negligent;
d) Whether Defendant timely informed Plaintiffs of the Data Breach;
e) Whether Plaintiffs and Class Members are entitled to injunctive relief; and
f) Whether, as a result of Defendant's conduct, Plaintiffs and the Class are entitled to damages and equitable relief.

34. **Typicality:** Plaintiffs' claims are typical of the Class Members' claims because all Class Members were comparably injured through Defendant's substantially uniform misconduct described above. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other members of the Class that they seek to represent, and there are no defenses that are unique to either Plaintiff. Plaintiffs and Class Members' claims and injuries arise from the same facts and are based on the same law.

35. **Adequacy:** Plaintiffs are an adequate Class Representative because their interests do not conflict with the interests of other Class Members they seek to represent; Plaintiffs have retained competent counsel that is experienced in complex class action litigation; and Plaintiffs intend to vigorously prosecute this action. The interests of Class Members will be fairly and adequately protected by Plaintiffs and their counsel.

36. **Superiority:** A class action is superior to other available methods for fair and efficient adjudication of this controversy. No unusual difficulties are likely to be encountered in the management of this class action. The damages suffered by Class Members are relatively small compared to the expense required to individually litigate their claims against Defendant, so it would be virtually impossible for the Class Members to seek individual redress against Defendant's wrongful conduct.

VI. CAUSES OF ACTION

COUNT ONE
NEGLIGENCE

37. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

38. Defendant owed Plaintiffs and Class Members a duty to exercise reasonable care in safeguarding their personal information, arising from the sensitivity of the information, the expectation the information was going to be kept private, and the foreseeability of its data safety shortcomings resulting in a breach. This duty included designing, implementing, maintaining, monitoring, and testing Defendant's protocols, policies, procedures, practices, networks, and systems to ensure Class Member information was sufficiently secure.

39. Defendant owed a duty to Plaintiffs and Class Members to implement administrative, physical, and technical safeguards, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiffs' and Class Members' PII. Defendant owed a duty to provide industry standard data security measures. Defendant owed a duty under Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, which prohibits the unfair practice of insufficient and unreasonable data protection measures.

40. Defendant owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII.

41. Defendant also had independent duties under Plaintiffs' and Class Members' state laws that require Defendant to reasonably protect Plaintiff's and Class Members' PII and promptly notify them about the breach.

42. Defendant and the Class entered into a special relationship when the Class Members entrusted Defendant to protect their Private Information, which provided an independent duty of care. Plaintiffs' and Class Members' willingness to entrust Defendant with their PII was

predicated on the understanding that Defendant would take adequate security precautions. Defendant was capable of protecting its networks and systems, and the PII it stored on them, from unauthorized access.

43. Defendant breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Plaintiffs' and Class Members' PII, including administrative, physical, and technical safeguards; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII.

44. Plaintiffs and Class Members were probable and foreseeable victims of Defendant's inadequate data security. Defendant knew, or should have known, of the risk of collecting and storing Plaintiffs' and Class Members' PII and the need for providing appropriate safeguards.

45. The harm to Plaintiffs and Class Members was a proximate, reasonably foreseeable result of Defendant's breaches of aforementioned duties.

46. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT TWO
NEGLIGENCE PER SE

47. Plaintiffs reallege and incorporate by reference paragraphs 1-36 as if fully set forth herein.

48. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate data security practices to safeguard Plaintiffs' and Class Members' PII.

49. Under state data security statutes, Defendant had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' PII.

50. Defendant breached its duties to Plaintiffs' and Class Members under the FTCA and state data security statutes by failing to provide fair, reasonable, or adequate data security practices to safeguard Plaintiffs' and Class Members' PII.

51. Plaintiffs and Class Members were foreseeable victims of Defendant's violations of the FTCA and state data security statutes. Defendant knew or should have known that its failure to implement reasonable security measures would cause damage to Plaintiffs and Class Members.

52. Defendant's failure to comply with applicable law constitutes negligence per se.

53. But for Defendant's violations of law, Plaintiffs' and Class Members' PII would not have been accessed by unauthorized parties.

54. Due to Defendant's violations of law, Plaintiffs and Class Members suffered injury of the type contemplated by these laws, including, but not limited to, the exposure to a heightened and imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring, and other protective measures to detect or deter identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished the value of their PII.

55. The harm to Plaintiffs and Class Members was a proximate, reasonably foreseeable result of Defendant's breaches of applicable law.

56. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT THREE
UNJUST ENRICHMENT

57. Plaintiffs reallege and incorporate by reference paragraphs 1-36 as if fully set forth

herein.

58. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of monetary payments – directly or indirectly – for services received.

59. Defendant collected, maintained, and stored the PII of Plaintiffs and Class Members, and, as such, Defendant had knowledge of the monetary benefits conferred by Plaintiffs and Class Members.

60. The money paid to Defendant in connection with services provided concerning Plaintiffs' PII should have been used to pay, at least in part, for the administrative costs and implementation of adequate data management and security. Defendant failed to implement – or adequately implement – practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

61. As a result of Defendant's failure to implement security practices, procedures, and programs to secure sensitive PII, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in the value between goods and services with reasonable data privacy that were paid to Defendant, and the services Defendant provided without reasonable data privacy.

62. Under principles of equity and good conscience, Defendant should not be permitted to retain money paid for services relating to Plaintiffs and Class Members because Defendant failed to implement the data management and security measures that are mandated by industry standards.

63. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds received by Defendant. A constructive trust should be imposed upon all unlawful and inequitable sums received by Defendant traceable

to Plaintiff and the Class.

COUNT FOUR
VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT
CAL. CIV. CODE SECTION 1798.150, *et seq.* ("CCPA")

64. Plaintiff Joseph Collins realleges and incorporates by reference paragraphs 1-36 as if fully set forth herein.

65. Plaintiff Joseph Collins is a resident of California.

66. Defendant collected California applicants' personal information as defined in Cal. Civ. Code § 1798.140.

67. By failing to protect Plaintiff's and Class Members' PII from theft, exfiltration, or unauthorized disclosure, Defendant breached its duties to ensure adequate data security practices and violated § 1798.150 of the CCPA.

68. Defendant had a duty to implement and maintain reasonable security measures to protect Plaintiff's and Class Members' PII. Defendant failed to do so.

69. Defendant's actions directly and proximately caused the unlawful distribution of Plaintiff's and Class Members' Private Information.

70. Plaintiff and Class Members seek equitable relief to ensure Defendant sufficiently secures applicants' PII by implementing sufficient data security procedures and practices. Defendant continues to hold applicants' PII. Plaintiff and Class Members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated its inability to sufficiently safeguard their information, demonstrated by the Data Breach.

71. An actual controversy now exists as to whether Defendant has implemented and maintained adequate security procedures and practices under the CCPA, in relation to the nature of the information.

72. Judicial intervention on this issue is necessary and appropriate under the

circumstances to prevent further data breaches of Plaintiff's and Class Members' PII.

73. Plaintiff and Class Members seek statutory damages or actual damages, including actual financial losses that are a result of the unlawful data breach.

COUNT FIVE
VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW BUSINESS & PROFESSIONS CODE SECTION 17200, *et seq*. ("UCL")

74. Plaintiff Joseph Collins realleges and incorporates the foregoing allegations as if fully set forth herein.

75. Plaintiff Collins is a resident of California.

76. Defendant is a "person" under the UCL, Cal. Bus. & Prof. Code § 17201.

77. Under California's UCL, Cal. Bus. & Prof. Code Section 17200, *et seq*., a business practice is "unfair" when "any injury it causes outweighs any benefits provide[d] to consumers and the injury is one that the consumers themselves could not reasonably avoid." *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

78. Defendant's failures to implement and maintain adequate security measures do not benefit applicants ("consumers"). Defendant implemented insufficient and ineffective security measures. Defendant diverted the funds necessary to ensure sufficient data security, which led to the Data Breach. Defendant did not follow protocols, policies, and procedures necessary for security and encryption in line with industry standards and requirements. Defendant concealed and omitted the material fact that it inadequately secured Plaintiff's and Class Members' PII. Defendant concealed and omitted the material fact that it did not fulfill its statutory obligations and common law duties for security of Plaintiff's and Class Members' PII. Defendant did not timely or adequately notify Plaintiff or Class Members about the Data Breach, its scope, or the information exfiltrated, such that they could not take appropriate mitigating steps to prevent identity theft and other harm.

79. Defendant was deceptive, misleading, and unreasonable, constituting an unfair business practice as interpreted by Cal. Bus. And Prof. Code Section 17200. Defendant's actions, as described herein, have resulted in harm to student applicants who paid for their applications to Defendant and whose practices were inconsistent with reasonable expectations of data security.

80. California's UCL finds a business practice is "unlawful" when Defendant breaches state or federal law and the "unfair competition law makes [these breaches] independently actionable." Defendant engaged in "unlawful" business practices by violating the FTC Act, 15 U.S.C. § 45, the CCPA, Cal. Civ. Code § 1798.100, and California Common Law.

81. Defendant's conduct, as alleged herein, is deceptive, misleading, unreasonable, and constitutes unlawful conduct. Defendant's conduct, including misrepresentations and omissions, was material because a regular applicant ("consumer") would be deceived about Defendant's data security standards. Defendant disregarded Plaintiff's and Class Members' rights. Defendant maliciously, intentionally, and knowingly violated California's Unfair Competition Law.

82. Defendant's unfair and unlawful conduct directly and proximately caused Plaintiff's and Class Members' injuries, including lost money or property. But for Defendant's unfair and unlawful acts, Plaintiff's and Class Members' harm would not have occurred, including an increased imminent risk of identity theft, a diminished value for their personal information, and necessary time and expenses for monitoring fraudulent activity. Due to Defendant's unlawful conduct, as alleged herein, applicants who entrusted their PII to Defendant have suffered injuries-in-fact as a result of the Data Breach.

83. Defendant's failure to enforce proper security measures violates public policy, which is designed to protect consumers' data and to ensure that organizations entrusted with such data adopt necessary security protocols. These objectives are reflected in laws such as the FTC

Act, 15 U.S.C. § 45, and the CCPA, Cal. Civ. Code § 1798.100. Consumers cannot reasonably avoid the injuries that Defendant caused as alleged herein. Victims' injuries outweigh the potential benefits to the Defendant. Defendant could have furthered its business interests in a manner other than this unfair conduct.

84. Plaintiff and Class Members seek an order enjoining Defendant from continuing its unlawful, deceptive, and unfair business practices. Plaintiff and Class Members seek an order requiring Defendant to implement and maintain sufficient data security practices in accordance with its statutory and common law duties. Plaintiff and Class Members request an award for restitution for the money wrongfully acquired by Defendant's unfair and unlawful practices.

COUNT SIX
VIOLATION OF THE CONSUMER LEGAL REMEDIES ACT
CALIFORNIA CIVIL CODE SECTION 1750, *et seq*. ("CLRA")

85. Plaintiff Joseph Collins realleges and incorporates the foregoing allegations as if fully set forth herein.

86. The CLRA prohibits "unfair methods of competition and unfair or deceptive acts or practices" in connection with the sale of services. Cal. Civ. Code § 1770.

87. Defendant's unlawful conduct described herein was intended to increase applications ("sales") by prospective students ("the consuming public") and violated Section 1770(a)(5), (a)(7) and (a)(9) of the CLRA by representing that the products and services have characteristics and benefits, such as appropriate data security, that it does not have.

88. Defendant fraudulently deceived Plaintiff and the California Class by representing that its application process ("products and services") had certain characteristics, benefits, and qualities which it does not have, namely data protection and security. In doing so, Defendant intentionally misrepresented and concealed material facts from Plaintiff and the Class, specifically by advertising secure services when Defendant in fact failed to institute adequate security measures

and neglected system vulnerabilities that led to a data breach. Said misrepresentations and concealment were done with the intention of deceiving Plaintiff and the Class and depriving them of their legal rights and money.

89. Defendant's claims about the products and services led and continues to lead consumers like Plaintiff to reasonably believe that Defendant has implemented adequate data security measures when Defendant in fact neglected system vulnerabilities that led to a data breach and enabled hackers to access customers' PII.

90. Defendant knew or should have known that adequate security measures were not in place and that consumers' PII was vulnerable to a data breach. Plaintiff and the California Class have suffered injury in fact as a result of and in reliance upon Defendant's false representations. Plaintiff and the Class would not have purchased the products or used the services or would have paid significantly less for the products and services, had they known that their Personal Information was vulnerable to a data breach.

91. Defendant's actions as described herein were done with conscious disregard of Plaintiff and the rights of Class Members, and Defendant was wanton and malicious in its concealment of the same.

92. Plaintiff and the Class have suffered injury in fact and have lost money as a result of Defendant's unfair, unlawful, and fraudulent conduct. Specifically, Plaintiff paid for products and services advertised as secure, and consequentially entrusted Defendant with his PII, when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiff and the Class would not have purchased the products or services, or would not have provided Defendant with their PII, had they known their Personal Information was vulnerable to a data breach.

93. Defendant should be compelled to implement adequate security practices to protect customers' PII. Additionally, Plaintiff and the Class Members lost money as a result of Defendant's unlawful practices.

94. Plaintiff and the Class Members seek all monetary and nonmonetary relief allowed by law including restitution; reasonable attorneys' fees and costs under California Code of Civil Procedures § 1021.5; and injunctive relief under the CLRA pursuant to Cal. Civ. Code 1782(d) and other appropriate equitable relief.

COUNT EIGHT
DECLARATORY JUDGMENT

95. Plaintiffs reallege and incorporate by reference paragraphs 1-36 as if fully set forth herein.

96. Plaintiffs and the Class have stated claims against Defendant based on negligence, negligence per se, and unjust enrichment.

97. Defendant failed to fulfill its obligations to provide adequate and reasonable security measures for the PII of Plaintiffs and the Class, as evidenced by the Data Breach.

98. Due to the Data Breach, Defendant's systems are more vulnerable to unauthorized access and require more stringent measures to be taken to safeguard the PII of Plaintiffs and the Class moving forward.

99. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's current obligations to provide reasonable data security to protect the PII of Plaintiffs and the Class. Defendant maintains that its security measures were – and still are – reasonably adequate and denies that it previously had or have any obligation to implement better safeguards to protect the PII of Plaintiffs and the Class. Specifically, Plaintiffs and the Class seek a declaration that Defendant's existing security measures do not comply with its obligations, and that Defendant

must implement and maintain reasonable security measures to comply with its data security obligations.

PRAYER FOR RELIEF

100. Plaintiffs, on behalf of themselves and on behalf of the proposed Class, request that the Court:

a) Certify this case as a class action, appoint Plaintiffs as class representatives, and appoint Plaintiffs' Counsel as Class Counsel for Plaintiffs to represent the Class;

b) Find that NYU breached its duties to safeguard and protect the PII of Plaintiffs and Class Members that was compromised in the Data Breach;

c) Award Plaintiffs and Class Members appropriate relief, including actual and statutory damages, restitution and disgorgement;

d) Award equitable, injunctive and declaratory relief as may be appropriate;

e) Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

f) Award pre-judgment and post-judgment interest as prescribed by law; and

g) Grant additional legal or equitable relief as this Court may find just and proper.

DATED: March 28, 2025

Respectfully Submitted,

/s/ Jonathan D. Lindenfeld
Jonathan D. Lindenfeld, # JL1990
FEGAN SCOTT LLC
305 Broadway, 7th Floor
New York, NY 10007
Phone: 332.216.2101
Fax: 312.264.0100
jonathan@feganscott.com

Elizabeth A. Fegan (*pro hac vice to be filed*)
Megan A. Shannon (*pro hac vice to be filed*)
FEGAN SCOTT LLC
150 S. Wacker Dr., 24th Floor
Chicago, IL 60606
312-741-1019
Beth@feganscott.com
Megan@feganscott.com

COTCHETT, PITRE & MCCARTHY, LLP
Thomas E. Loeser (*pro hac vice to be filed*)
Karin B. Swope (*pro hac vice to be filed*)
Vara G. Lyons, NY Bar # 5464524
Attorneys for Plaintiffs
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Telephone: (206)-802-1272
Facsimile: (206)-299-4184
tloeser@cpmlegal.com
vlyons@cpmlegal.com

Attorneys for Plaintiffs and the Proposed Class